процеси / О. М. Максимова; Миколаїв. держ. гуманіт. ун-т ім. П. Могили. – Миколаїв, 2007. – 18 с.
5. Політологічний енциклопедичний словник / Упорядник В. П. Горбатенко; За ред. Ю. С. Шемшученка, В. Д. Бабкіна, В. П. Горбатенка. – К.: Генеза, 2004. – 736 с.
6. **Работяжев Н. В.** Механизмы рекрутирования и воспроизводства политической элиты в посткоммунистической России / Н. В. Работяжев. – Режим доступа: http://ecsocman.hse.ru/data/673/685/1219/003Rabotyazhev.pdf
7. **Rosenberger S. K.** Participatory Elites? (In-)Equality of Political Participation in Austria / S. K. Rosenberger, F. Walter. – Режим доступу: http://homepage.univie.ac.at/ florian.walter/PARTEL/Homepage/Texte/Outline Ine qualitv%20oP/o20political%20 Participation%20in%20Austria.pdf

Надійшла до редколегії 14.05.2012 р.

УДК 327.8

Г. Г. Четверик
Дніпропетровський національний університет імені Олеся Гончара

НАПРЯМКИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Здійснюється дослідження значимості можливих кібернетичних та мережевих загроз для держави. Визначаються напрямки державної політики, спрямованої на упередження таких загроз. Описуються основні характеристики кожного з напрямків.
Ключові слова: кібернетична безпека, Інтернет, мережі, соціальні мережі.

Осуществляется исследование значимости возможных кибернетических и сетевых угроз для государства. Определяются направления государственной политики, направленной на предупреждение таких угроз. Описываются основные характеристики каждого из направлений.
Ключевые слова: кибернетическая безопасность, Интернет, сети, социальные сети.

The paper is study the significance of possible cyber threats and network for the state. Determine the areas of public policy aimed at preventing such threats. Main characteristics of each of the directions are describes.
Keywords: cyber security, Internet, networks, social nets.

Актуальність. Важливість кіберпростору для життя сучасного суспільства є очевидною, зважаючи не тільки на такі показники, як кількість користувачів мережі Інтернет та динаміка їх збільшення, але й поступове проникнення його у решту сфер людського життя. Наука, економіка, культура були першими, хто відчули спочатку зиск від використання мережевих можливостей та технологій, а згодом – свою залежність від умов їх використання. Наразі використання мережевих можливостей та технологій стає все більш очевидним для політики і безпеки держави. «Якщо у світі сьогодні ще зберігається стратегічний баланс у сфері звичайних озброєнь та зброї масового знищення, то питання паритету в кіберпросторі залишається відкритим. Підтвердженням цього є активність спеціальних підрозділів окремих держав, громадських і терористичних організацій, яка націлена на використання кіберпростору для досягнення різноманітних політичних, економічних та військових цілей» [1]. Промовистими свідченнями важливості мережевих технологій є також так звані «кольорові» революції, події «арабської війни» та численні кризи, що відбувалися у багатьох країнах світу. Тому актуальним завданням є визначення можливостей державної політики у сфері протидії кібернетичним загрозам і формування умов, що

сприятимуть кібернетичній безпеці. Реалізацією подібних завдань повинні займатися не тільки фахівці з питань безпеки, кібернетики, комунікацій, але й політологи, оскільки вони мають визначитися з загальним напрямком протидії держав подібного типу загрозам. Відтак мета даної статті: визначити напрямки державної політики у сфері кібернетичної безпеки.

Основна частина. Питання кібернетичної безпеки вже стало предметом дослідження українських учених. Проте звертають на нього увагу, в першу чергу, фахівці з питань національної безпеки [7] та представники юридичної науки, зокрема О. Мережко [6, с. 94–95], а політологічних досліджень цієї проблематики практично немає. Поширеними є дослідження можливостей використання мережевих технологій у рамках електоральних процесів, партійного будівництва, іміджбілдингу тощо. Тобто увага політологів прикута до питання використання можливостей мереж в рамках передвиборних кампаній, «розкрути» політичного лідера чи партійного проекту, тоді як більш глобальні питання, такі як їх вплив на політичну стабільність держави, можливі реакції держави на загрози подібного характеру та походження, залишаються поки що поза увагою науковців. Натомість все більш пильну увагу цьому питанню проявляють військові, правоохоронці та державні урядовці. Зокрема високопосадовці США та експерти, задіяні в підготовці нової «Стратегічної концепції НАТО», наголошували на необхідності розглядати кібернапади на критичноважливу інфраструктуру як «акт війни» [7] з відповідною реакцією зі сторони країн Блоку.

На сьогоднішній день близько двадцяти держав знаходяться в процесі трансформації власних військових потенціалів з огляду на можливості використання мережі Інтернет. Формуються спецпідрозділи, які мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника. Згідно з офіційними заявами, такі підрозділи створено в США (U. S. Cyber Command), Великобританії (Cyber Security Operations Centre), Німеччині (Internet Crime Unit та Federal Office for Information Security), Австралії (The Cyber security operations centre), Індії та інших державах. Активну позицію щодо протидії кіберзагрозам займає і провідна міжнародна безпекова організація – НАТО (Cooperative Cyber Defence Centre of Excellence).

Мілітаризацію кіберпростору можна вважати одним з найбільш очевидних та важливих напрямків державної політики у цій сфері. Незважаючи на декларовані бажання міжнародних організацій, таких як ООН, та більшості основних геополітичних суб'єктів протидіяти його мілітаризації, можна очікувати подальшого розвитку наступальних та оборонних засобів ведення війни у кіберпросторі, зважаючи на їх потенційну ефективність, аж до виникнення нової «гонки озброєнь» до створення засобів ведення кібервійн, а також зростання кількості випадків використання мережевих можливостей та технічних потужностей розвідувальними службами та транснаціональними кримінальними групами, що спеціалізуються у сфері кіберзлочинності, змушує уряди держав переглядати і свою внутрішню політику в кіберсфері. Наприклад, помітною є активністю у сфері кібербезпеки відрізняється Адміністрація Б. Обами. Після обрання на посаду було оприлюднено «Огляд кібербезпеки» (Cyber Security Review) – комплексний документ, що визначає основні пріоритети нової команди у сфері кібербезпеки; створено посаду Керівника Кібербезпеки Ради національної та внутрішньої безпеки; оприлюднено нову «Стратегію національної безпеки» (2010), в якій кіберзагрозам вперше відведено окреме місце в загальній структурі загроз США; було збільшено держзамовлення на розробку кіберозброєнь та нових, більш захищених, військових мереж; створено проекти нормативних документів, що спрямовані на покращення взаємодії в сфері кібербезпеки союзниками США та убезпечення власного Інтернет-простору в разі виникнення ситуацій, що загрожують національній безпеці. Також в США розглядається можливість ухвалення закону, на базі якого буде створено «інститут національного радника у справах кібербезпеки, котрий буде займатися цими питаннями в рамках Національного Агентства Безпеки, повітряних силах, Департаменті Національної Безпеки, а також в інших державних структурах. Відповідний закон передбачає вельми широкі повноваження для цього радника, у

тому числі дає йому право виключати федеральні мережі у випадку «серйозної загрози» [6, с. 94]. Таким чином, другий напрямок державної політики у сфері кібернетичної безпеки можна назвати структурним, оскільки він полягає у розвиткові нових структур відповідного напрямку та створенні окремих підрозділів у рамках традиційних інститутів.

Цікаво, що в деяких країнах НАТО, наприклад в Естонії, говориться про необхідність впровадження спеціальних предметів з кібербезпеки навіть у школі [9, с. 40]. Подібні заходи є цілком виправданими, зважаючи на такі явища як «кібербуллінг» [4, с. 10], Інтернет-залежність [3] та інші загрози проблеми, наприклад: медико-біологічні; проблеми соціальної адаптації та психологічної адаптації до опанування інформацією; проблеми з мережевою анонімністю та приватністю [8]. Тому наступним напрямком державної політики у сфері кібернетичної безпеки можна назвати освітній. Відповідні заходи, наприклад, шкільні предмети та заходи, які мають знизити ризик індивідуальних кіберзагроз, повинні становити важливий напрямок державної політики.

У деяких випадках державна політики протидії кіберзагрозам викликає дискусії, які стосуються основоположних питань політичної філософії, зокрема, про права громадянина, особисту свободу і приватність, державний суверенітет тощо. Завдання протидії порушенню авторських прав, розповсюдженню дитячої порнографії, боротьби з комп'ютерним піратством та зростанням терористичної загрози виконується державними органами через впровадження моніторингової, лімітуючої та, певною мірою, цензурної політики. Практично кожна з країн, що має відповідні технічні можливості, використовує мережу Інтернет моніторингу інформаційних потоків чи, простіше кажучи, відстежування змісту веб-сайтів, електронної пошти, інформаційних запитів тощо. Зусиллями США, Великобританії, Канади. Австралії та Нової Зеландії було створено систему «Ешелон», яка перехоплює за допомогою супутників повідомлення, що проходять телефонними лініями, радіо, супутниковим зв'язком та аналізує їх зміст на предмет присутності підозрілих слів та висловів. Існування цієї системи приховувалося, і тільки після того, як 21 жовтня 1999 р. рух «Хактивісти» провів «День боротьби з «Ешелоном» (вони пересилали якимога більше листів із словами «революція», «плутоній», «Північна Корея», «ЦРУ» тощо), Австралія визнала його існування [4]. У Великобританії був прийнятий закон, згідно з яким уряд отримав право відстежувати електронну пошту громадян та декодувати криптовані повідомлення. До офісу новоствореної установи, Урядового Центру технічної підтримки, провайдери будуть зобов'язані протягнути виділену лінію за кошти державного бюджету. Під тиском громадськості була прийнята поправка Палати лордів, згідно з якою на перехоплення e-mail буде потрібна санкція прослуховування. Але, якщо спецслужби самі не зможуть розшифрувати якесь повідомлення, новий закон зобов'язує користувачів надавати паролі для розшифрування своїх листів [2].

Країни з авторитарними політичними режимами достатньо активно застосовують не тільки моніторинг чи обмеження, але й методи цензури, прямого впливу та тиску на власників пошукових Інтернет-сервісів, де або розміщуються матеріали, що викликають невдоволення з боку державних інституцій, або ж які надають доступ до таких матеріалів. Лідером у цьому вважається Китай. Найбільш показовим у цьому контексті є конфлікт між урядом Китаю та IT-корпорацією Google, який виник через небажання Google обмежувати на вимогу уряду пошукові запити китайських користувачів [7].

Незважаючи на те, що безпосередньою причиною виникнення конфліктної ситуації між урядом КНР та Google стала спроба китайських хакерів на початку 2010 року здійснити злам електронних поштових скриньок, що належать деяким китайським правозахисникам, саме «цензурна проблема» призвела до відкритого конфлікту. Корпорація Google прагне боротися з «цензурними проблемами» за допомогою сервісу «Transparency Report», який має висвітлювати, як часто держави звертаються до корпорації з запитами про усунення того чи іншого контенту або про надання доступу до персональних даних користувачів сервісів корпорації. Результати, оприлюднені корпорацією, виявилися дещо несподіваними. Згідно з даним звітом саме демократичні крани Заходу (США та країни ЄС) є в

цілому лідерами з таких запитів. Наприклад, лише за період з січня 2010 року до липня 2010 року [10] уряд США звертався до корпорації з подібними запитами 4287, Великобританії – 1343, Франції – 1017, Німеччини – 668, Італії – 651, Іспанії – 372, Португалії – 73, Бельгії – 71. Не менш активними в даній сфері є і країни БРІК (крім Росії – кількість звернень менше 10): Бразилія зверталась із 2435 запитами, Індія – 1430. Дані про Китай корпорація не розкриває, посилаючись на те, що Китай вважає цензурні вимоги частиною державної таємниці.

Відомо, що КНР цензурує аудіо- та відеоконтент сервісів, подібних до «YouTube», починаючи з 2008 року. Дана проблема навіть стала причиною розробки нових регулятивних правил із розміщення відеоконтенту на китайських національних відеосервісах, які певною мірою ускладнюють можливість неконтрольованого розміщення аудіо- та відеоматеріалів у широкодоступних мережах. КНР чітко пов'язало безконтрольність розміщення відео- та аудіоматеріалів із загрозами єдності та суверенітету Китаю, завдання шкоди етнічній солідарності, пропагування насилля та порнографії, порушенням прав особи, завдання шкоди китайській культурі чи традиціям [7]. Хоча країни Заходу намагаються безпосередньо не втручатись у діяльність подібних сервісів, однак свої претензії до деяких елементів контенту порталу YouTube висловлювали уряди Німеччини (через оприлюднення роликів, що пропагують нацистську ідеологію та антисемітизм), Великобританії (забезпечення можливостей для кібербуллінгу школярів), Росії (через розміщення екстремістських матеріалів).

Поширення мережі Інтернет і лавиноподібне збільшення кількості користувачів веде до зростання його значимості і в царині політики, зокрема масової політичної дії. Інтернет, наприклад, такі соціальні мережі, як Twitter або Facebook, дозволяють здійснювати широке поширення не тільки інформації, але й антиурядових матеріалів, закликів до непокори, повідомлень про масові акції непокори та місце і час зібрання активістів. З його появою не потрібно з ризиком для життя і великими витратами часу поширювати прокламації і розкидати листівки. Недаремно протести, що охопили мусульманський світ, були названі «твіттер-революцією». Значимість цієї соціальної мережі в організації акцій протесту і координації дій учасників була величезною. Інтернет виявився чудовим агітатором і організатором, і в цій якості він витісняє традиційні канали комунікації та ЗМІ. Тепер за допомогою соціальних мереж можна зібрати численний натовп з точністю до хвилин в потрібному місці під потрібними гаслами. Це технології. з якими держава майже не в змозі боротися і які мають подвійний вимір. З однієї сторони – це створює додаткові можливості для активістів громадянського суспільства у всьому світі, дозволяє опозиційним рухам в країнах з авторитарними режимами проводити ефективну діяльність, критикувати уряд і звертатися до своїх прихильників незважаючи на цензуру в традиційних ЗМІ, проте в Інтернеті також знаходить свій прилисток і непримиренна опозиція, рухи радикального, фашистського, націоналістичного типів. Наприклад, соціальній мережі Facebook загрожує мільярдний штраф через наявність сторінки під назвою «Третя палестинська інтифада». Інформація, що на ній міститься, являє собою антиізраїльську пропаганду і заклики до насильства. Ця сторінка була достатньо швидко видалена, але її встигли прочитати більше ніж півмільйона користувачів [5]. В Інтернеті можна знайти політичні та екстремістські заклики, проповіді представників тоталітарних культів та сект, фетви, пряму дезінформацію, майстерну брехню. Це змушує всі держави до певного лімітування та цензурування мережевих ресурсів.

Такий підхід демократичних країн у сфері внутрішнього інформаційного (кіберпростору) все частіше набуває окремих рис політики тих країн, що традиційно відносять до авторитарних, хоча і з певними суттєвими відмінностями. Якщо в країнах авторитарного типу спостерігається політика, в першу чергу, прямого обмеження доступу, то країни Заходу йдуть шляхом нарощування кількості даних про користувачів, моніторингу в першу чергу національного Інтернет-трафіку та отриманню можливостей цільового відключення окремих елементів Мережі чи її користувачів. Такий акцент на «моніторинговому дискурсі» обумовлений, в тому числі, зростанням кількості телекомунікаційних послуг та мереж, контроль за якими значною мірою ускладнено для державних правоохоронних служб [7].

Ці зусилля держав викликають заперечення зі сторони громадськості і породжують звинувачення в придушенні свободи слова та обмеженнях прав громадян, актуалізують питання про баланс між вільним інформаційним потоком і захистом громадських та особистих інтересів.

Проте держава є не тільки порушником прав людини в кіберпросторі, але й захисником. Окремим напрямком державної політики має бути захист прав користувачів Інтернету, які порушуються з комерційною метою. Наприклад, багато компаній передають користувачам, коли ті відвідують їх сайти, так звані «cookies». Це невеликі приховані програми, які відстежують інтереси користувача (до яких сайтів він звертається) і пересилають ці дані до своєї компанії, яка використовує їх для прямої реклами (тобто реклами певних товарів тільки тим людям, яких ці товари можуть зацікавити). Подібна діяльність сама потребує контролю зі сторони держави. Практика поступової актуалізації участі державних органів у функціонуванні мережі Інтернет та посилення їх моніторингових та контролюючих функцій вже практично не зустрічає опору навіть у тих країнах, де існує активний контроль за збереженням демократичних свобод. За результатами опитування компанії Sophos, більшість американців не бачать проблем із тим, що уряд використовує технології для моніторингу та фільтрації мережевого трафіку, а також має доступ до поштових серверів. Опитані стверджують, що не проти доступу спецслужб до їх пошти [7].

Висновки. Однією з головних тенденцій сучасності є мілітаризація кіберпростору, яка виражається в розвитку різноманітних наступальних та оборонних засобів ведення війни у кіберпросторі, трансформації військових потенціалів держав з огляду на можливості використання мережі Інтернет, в напрямку формування спецпідрозділів, які мають на меті: ведення розвідувальної роботи в мережах, захист власних мереж, блокування і «обвал» структур супротивника. Мілітаризація, яка є наслідком зусиль декількох держав, відбивається на загальному стані кіберпростору і впливає на кібернетичну безпеку усіх без винятку держав, змушуючи їх до пошуку адекватних відповідей. Одним з варіантів цієї відповіді є другий напрямок державної політики у сфері кібернетичної безпеки, який можна назвати структурним, оскільки він полягає у розвиткові державних структур відповідного спрямування. Проте для гарантування індивідуальної безпеки громадян у цьому напрямку створення державних структур недостатньо. Крім того, це не обов'язково буде й найбільш ефективним засобом, зважаючи на ті можливості, які надає освітній напрямок у державній політиці кібербезпеки. Полягає він у поширенні комп'ютерної грамотності та підготовці користувачів мережі Інтернет до різноманітних загроз та небезпек, які вона містить.

Підсумовуючи дослідження напрямків державної політики у сфері кібернетичної безпеки, можемо зазначити, що глобальним трендом цього напрямку є посилення контролю з боку державних органів за контентом національного інформаційного простору, за мережевим трафіком, засобами доступу до всесвітньої мережі Інтернет, яке здійснюється шляхом налагодження та здійснення моніторингу, лімітування та цензурування. Подібна політика держави знову актуалізує питання про співвідношення класичних прав та обов'язків громадянина та держави в просторі мережі Інтернет та формування своєрідних «цифрових» чи «інформаційних суверенітетів». Останнє поняття може зрештою перетворитися на одне з ключових питань кібернетичної безпеки держави. В рамки цього поняття входить багато що. В першу чергу це, звісно, власна операційна система, власні пошукові й інформаційні системи, антивірусні, шифрування, кореневий домен, свій процесор, власна система геопозиціонування. На даний момент єдиною країною, яка володіє повноцінним «цифровим суверенітетом», є США, що викликає природне занепокоєння інших країн. Зокрема китайські вчені запропонували ввести та легітимізувати у міжнародному праві поняття «інтернет-кордон» та «інтернет-суверенітет», Президент Казахстану Н. Назарбаєв висунув практично аналогічну пропозицію про визначення «електронного кордону» та «електронного суверенітету». Розглядаючи зазначену тенденцію разом із можливістю зменшення рівня анонімності у всесвітній мережі (із введенням «Інтернет-паспорта» для користувачів), можна зазначити, що панівний до останнього часу неоліберальний підхід до розуміння мережі Інтернет (так звана «Каліфорнійська ідеологія», до якої Р. Барбрук та А. Камерон відносили: 1) пропагування «віртуального класу» –

«техноінтелігенції з вчених, інженерів, комп'ютерних вчених, розробників відеоігор та інших фахівців в сфері комунікацій»; 2) виникнення «вільного цифрового ринку»; 3) виникнення «цифрової Агори») зазнає кардинальних змін, а на зміну йому приходить «технореалізм» з ключовою роллю держави у розвитку мережі Інтернет (А. Шапіро, Д. Шенк, С. Джонсон). Для «технореалізму» технології не є нейтральними, держава відіграє важливу роль у формуванні нового електронного світу, вона не лише має право, а й зобов'язана допомогти інтегрувати кіберпростір та звичне суспільство, інформація «хоче» бути захищеною.

Бібліографічні посилання

1. **Даник Ю.** Полігон протистояння – кіберпростір [Електронний ресурс] / Юрій Даник. – Режим доступу: http://na.mil.gov.ua/number/4837/1915.htm
2. **Іванов В.** Інформаційна безпека України: аспект діяльності ЗМК [Електронний ресурс] / В. Іванов. – Режим доступу: http://journlib.univ.kiev.ua/index.php?act=article& article= 1921.
3. Інтернет-залежність як новий феномен сучасного світу: сутність і проблеми. – К.: НІСД, 2011. – 47 с.
4. Кібербезпека: світові тенденції та виклики для України. – К.: НІСД, 2011. – 30 с.
5. Кібервійни – міф чи реальність? [Електронний ресурс]. – Режим доступу: http://nano.if.ua/page/kiber-vijni-mif-chi-realnist
6. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка / [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/294/
7. **Мережко О.** Проблеми кібервійни та кібербезпеки в міжнародному праві [Текст] / Олександр Мережко // Юридичний журнал. – 2009. – № 6. – С. 94–95.
8. Щодо основних викликів безпеці особи в умовах стрімкого впровадження сучасних інформаційних технологій. Аналітична записка [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/531/
9. **Morozow J.** Wrog z sieci / J. Morozow // Newsweek. – 24.05.2009. – S. 40–41.
10. Transparency Report: Government Requests [Електронний ресурс]. – Режим доступу: http://www.google.com/transparencyreport/governmentrequests/

Надійшла до редколегії 28.02.2012 р.

УДК 321.323

В. М. Щербак
Дніпропетровського національного університету імені Олеся Гончара

ПОЛІТИЧНЕ РЕКРУТУВАННЯ В КОНТЕКСТІ ЗАВДАНЬ ДЕМОКРАТИЗАЦІЇ: НАПРЯМКИ ПЕРЕТВОРЕННЯ ВИКОНАВЧОЇ ВЛАДИ

Розглядаються проблеми і перспективи демократичної трансформації політичного рекрутування. Аналізуються теоретичні передумови партійного і державного кадрового менеджменту. Встановлюються тенденції взаємодії держави і громадянського суспільства в межах реалізації політичного рекрутування.

Ключові слова: політичне рекрутування, демократизація, громадськість, вертикальна мобільність, ієрархія, мережний принцип.

Рассматриваются проблемы и перспективы демократической трансформации политического рекрутирования. Анализируются теоретические предпосылки партийного и государственного кадрового менеджмента. Устанавливаются тенденции взаимодействия государства и гражданского общества в рамках реализации политического рекрутирования.